CERTCHAIN: A BLOCKCHAIN-BASED CERTIFICATE AUTHENTICATION SYSTEM USING SMART CONTRACTS AND AI-BASED VERIFICATION

[1]Neha Beegam P E, [2]Alen K Sangeeth, [3]Athulraj Appukuttan, [4]Alex Jo Tomy, [5]Alex Rijo Joseph
[1]Assistant Professor, [2,3,4,5]Student
Department of Computer Science and Engineering,
[1,2,3,4,5]Federal Institute of Science and Technology (FISAT),
Mookkannoor, Kerala, India

***Abstract*—With the rapid digital transformation of educational and professional environments, certificate verification has become a critical security concern. Traditional certificate authentication systems rely on centralized repositories and manual validation processes, making them vulnerable to forgery, unauthorized modification, and operational inefficiencies. To address these challenges, this paper presents CertChain, a blockchain-based certificate authentication system that ensures secure, decentralized, and tamper-proof credential verification. The proposed sys- tem integrates Ethereum smart contracts, cryptographic hashing, and off-chain storage mechanisms to enable immutable certificate management. In addition, a decentralized governance mechanism is introduced to validate institutions through majority voting, ensuring trust and authenticity in certificate issuance. The system further incorporates AI-based modules for identity verification and automated marklist extraction, enhancing accuracy and preventing fraudulent activities such as deepfakes and proxy registrations. Certificates are generated as digital documents, hashed using SHA-256, and stored on the blockchain, allowing real-time verification by comparing cryptographic signatures. Experimental analysis demonstrates that the proposed system significantly reduces verification time, improves security, and eliminates dependency on centralized authorities. The integration of blockchain, artificial intelligence, and decentralized governance makes CertChain a scalable and robust solution for next- generation credential authentication systems.**

***Index Terms*—Blockchain, Certificate Authentication, Ethereum, Smart Contracts, AI Verification**

I. INTRODUCTION

The rapid digitalization of education and recruitment ecosystems has led to an increasing reliance on digital certifi cates for validating academic qualifications and professional competencies. With the growth of online learning platforms, remote hiring, and global mobility, the need for secure and efficient certificate verification mechanisms has become more critical than ever. However, traditional certificate authentication systems are predominantly centralized and rely on manual verification processes, which introduce several challenges including certificate forgery, unauthorized modifications, lack of transparency, and significant verification delays.

Centralized repositories are particularly vulnerable to single points of failure, insider attacks, and large-scale data breaches. In many real-world scenarios, verification requires direct communication with issuing institutions, leading to increased administrative overhead and inefficiency. Furthermore, the absence of standardized and globally accessible verification frameworks makes cross-institutional validation difficult and time-consuming.

Blockchain technology has emerged as a transformative solution to these challenges by offering a decentralized, immutable, and transparent data management framework. Through the use of cryptographic hashing, distributed ledgers, and consensus mechanisms, blockchain ensures data integrity and eliminates the possibility of tampering. Smart contracts enable automated certificate issuance, validation, and revocation without the need for intermediaries, thereby improving efficiency and trust.

Despite these advantages, existing blockchain-based certificate authentication systems exhibit several limitations. Many solutions focus primarily on storing certificate hashes on- chain without addressing critical aspects such as issuer validation, user identity verification, and real-world deployment challenges. Public blockchain implementations often suffer from high transaction costs and latency, while permissioned systems may compromise decentralization and transparency. Additionally, most existing approaches lack intelligent automation mechanisms for processing academic data and detecting fraudulent activities.

To overcome these limitations, this paper proposes **CertChain**, a comprehensive and scalable blockchain-based certificate authentication system that integrates decentralized governance, artificial intelligence, and secure storage mechanisms. Unlike conventional approaches, CertChain introduces a democratic voting-based governance model to verify and authorize institutions before allowing them to issue certificates. This ensures that only trusted entities participate in the ecosystem, enhancing overall system credibility.The proposed system further incorporates AI-based modules for identity verification and automated marklist extraction. Facial recognition techniques are employed to prevent impersonation and deepfake-based fraud, while natural language processing methods are used to extract and validate academic data from uploaded marklists. These intelligent components

significantly reduce manual intervention and improve data accuracy.In CertChain, certificates are generated as digital documents and hashed using the SHA-256 cryptographic algorithm. The hash is then stored on the Ethereum Sepolia blockchain using smart contracts, ensuring immutability and tamper resistance. To optimize storage efficiency, actual certificate files are maintained using off-chain storage mechanisms, while the blockchain stores only essential metadata and cryptographic proofs. Verification is performed by recomputing and matching hashes, enabling real-time authentication without requiring interaction with issuing institutions.

The system also supports role-based access control, secure authentication using JWT, and seamless integration with Web3 wallets such as MetaMask for transaction signing. Public users, including employers and verification agencies, can independently verify certificates using unique certificate identifiers, ensuring transparency and accessibility.

The major contributions of this work are summarized as follows:

- Design and development of a decentralized certificate authentication system using blockchain technology.
- Introduction of a governance-based institution verification mechanism using majority voting.
- Integration of artificial intelligence for identity verification and automated academic data extraction.
- Implementation of a hybrid storage model combining blockchain and off-chain systems for scalability.
- Development of a secure, transparent, and efficient verification framework that eliminates dependency on centralized authorities.

II. Related Work

A comprehensive overview of blockchain-based certificate authentication systems is presented in our previous work [1]. The study systematically analyzes existing approaches by examining different blockchain architectures, including public, consortium, and permissioned networks, along with their respective advantages and limitations. It also evaluates the role of smart contracts in automating certificate issuance and verification, and the use of cryptographic hashing techniques to ensure data integrity and immutability.

The survey highlights that traditional certificate authentication systems rely heavily on centralized databases and manual verification processes, which are prone to security vulnerabilities such as certificate forgery, unauthorized modification, and data breaches. Additionally, these systems suffer from operational inefficiencies, including high verification time, lack of transparency, and dependency on issuing authorities for validation.

Furthermore, the study explores various storage mechanisms adopted in blockchain-based systems, including on-chain storage and hybrid approaches using off-chain solutions such as IPFS. It emphasizes the trade-offs between storage efficiency, cost, and scalability. The analysis also considers performance metrics such as transaction cost, verification latency, throughput, and storage overhead, providing a comparative understanding of different system designs.

The survey identifies several critical research gaps that remain unresolved in existing solutions. These include scalability limitations in public blockchain systems, high trans- action costs associated with smart contract execution, lack of interoperability across different blockchain platforms, and insufficient mechanisms for issuer validation and trust management. Moreover, most existing systems lack intelligent automation features such as identity verification and automated data extraction, which are essential for real-world deployment. Overall, the findings of this survey provide a strong foundation for the development of advanced certificate authentication systems. They highlight the need for a comprehensive solution that integrates blockchain with decentralized governance, efficient storage mechanisms, and intelligent verification techniques, which motivates the design of the proposed CertChain system.

Fig. 1. General Architecture of Blockchain-Based Certificate Authentication Systems

A. Ethereum-Based Certificate Authentication Systems

R. Priyadarshini et al. [2] proposed a blockchain-based certificate authentication system using Ethereum smart contracts. The system stores cryptographic hashes of certificates on the blockchain, ensuring immutability and tamper-proof verification. To enhance verification efficiency, Bloom Filters are incorporated, enabling faster search and membership checking without exhaustive comparisons.

The framework introduces a dual-layer validation mechanism, where both the certificate authenticity and the legitimacy of the issuing authority are verified. Smart contracts auto- mate certificate issuance and validation processes, reducing dependency on centralized authorities and improving system transparency. Experimental results indicate improved verification speed, reduced search time, and enhanced resistance to certificate forgery compared to traditional approaches.

However, the system relies on a public blockchain infrastructure, which introduces challenges such as high gas costs, increased transaction latency, and scalability limitations during

periods of network congestion. Additionally, the system is primarily evaluated in controlled environments, and practical challenges related to large-scale deployment and real-world integration are not fully addressed.

Fig. 2. Ethereum-Based Certificate Authentication Framework

B. Digi-Physical Certificate Authentication Systems

S. Sharma et al. [4] proposed a digi-physical certificate authentication system that integrates blockchain technology with physical certificates using QR codes or embedded secure identifiers. In this approach, each physical certificate is tightly linked with its corresponding digital record stored on the blockchain through a unique cryptographic reference.

During certificate issuance, a digital certificate is generated and its cryptographic hash is stored on the blockchain using smart contracts. The physical certificate contains a QR code or secure tag that encodes this blockchain reference. During verification, the QR code is scanned to retrieve the blockchain record, and the hash of the presented certificate is compared with the stored hash to validate authenticity.

This approach effectively bridges the gap between physical and digital verification, making it highly resistant to both physical duplication and digital tampering. The system enables instant and decentralized verification without requiring direct interaction with the issuing authority, thereby improving efficiency and trust.

However, the system introduces higher deployment complexity due to the need for secure printing mechanisms, QR code generation, and physical–digital synchronization. Additionally, large-scale implementation may incur increased infrastructure and operational costs, making it less feasible for resource-constrained institutions.

TABLE I
SECURITY FEATURES OF DIGI-PHYSICAL SYSTEMS

Feature	Description
Forgery Resistance	Very High
Verification Speed	Fast
Deployment Cost	High

C. Permissioned Blockchain (Hyperledger) Systems

G. Ghani et al. [6] proposed a permissioned blockchain-based system using Hyperledger Fabric for managing academic credentials. In this framework, only authorized institutions participate as nodes in the network, ensuring controlled access and secure management of certificate data.

The system utilizes identity-based access control, where each participant is authenticated through a membership service provider (MSP). Certificates are digitally generated, and their cryptographic hashes are stored on the blockchain, ensuring data integrity and tamper resistance. Smart contracts, implemented as chaincode in Hyperledger Fabric, automate certificate issuance, verification, and update processes.

Unlike public blockchain systems, the permissioned architecture enables higher performance by reducing consensus complexity, resulting in low latency and high throughput. Additionally, the system enhances privacy by restricting data visibility to authorized participants, making it suitable for academic and institutional environments.

However, the system limits decentralization due to restricted participation and reliance on trusted entities. It also introduces administrative overhead in managing network governance, access control policies, and participant coordination. Furthermore, interoperability with other blockchain networks and large-scale deployment across diverse institutions remain challenging.

Fig. 3. Permissioned Blockchain Credential Management System

TABLE II
FEATURES OF PERMISSIONED BLOCKCHAIN SYSTEMS

Feature	Description
Access Control	Identity-based
Latency	Low
Throughput	High
Privacy	High
Decentralization	Limited

D. Privacy-Preserving Certificate Authentication Systems

A. Garba et al. [7] proposed a privacy-preserving certificate authentication system using cryptographic hashing and Bloom Filters. In this approach, sensitive certificate data is not stored

directly on the blockchain; instead, only cryptographic representations of the data are maintained, thereby minimizing the risk of information leakage.

The system employs Bloom Filters to enable efficient membership verification, allowing verifiers to check the existence of a certificate without accessing the original data. During verification, the hash of the certificate is compared against the Bloom Filter representation stored on the blockchain, ensuring both data integrity and privacy preservation.

This approach significantly reduces storage overhead and improves verification speed, as Bloom Filters allow constant-time membership checking. Additionally, the system eliminates the need for direct interaction with issuing authorities, enabling decentralized and privacy-aware verification.

However, the use of Bloom Filters introduces a probability of false positives, which may affect verification accuracy in certain cases. Furthermore, the system may require additional middleware or auxiliary components for verification, increasing system complexity. Key management and interoperability challenges are also not fully addressed, limiting large-scale deployment.

E. Summary of Limitations

Although existing systems provide significant improvements in certificate authentication, several limitations remain. Public blockchain systems suffer from high transaction costs, increased latency, and scalability challenges, especially under heavy network load. In contrast, permissioned blockchain systems offer improved performance and privacy but compromise decentralization and global transparency.

Furthermore, many existing approaches lack robust issuer validation mechanisms, making them vulnerable to unauthorized certificate issuance. Interoperability across different blockchain platforms is also limited, restricting seamless verification across institutions and systems. In addition, most solutions do not incorporate intelligent verification techniques such as identity authentication or automated data extraction, which are essential for ensuring real-world applicability.

Another critical challenge lies in storage and data management, where inefficient handling of on-chain and off-chain data can impact system performance and cost. User adoption and usability issues, including key management and interaction with blockchain interfaces, further hinder practical deployment. Moreover, the lack of standardized frameworks and regulatory guidelines further complicates large-scale adoption across different sectors.

These limitations highlight the need for a comprehensive, scalable, and intelligent certificate authentication framework. To address these challenges, the proposed CertChain system integrates blockchain technology with decentralized governance, artificial intelligence, and hybrid storage mechanisms to provide a secure, efficient, and tamper-proof solution for next- generation credential verification. This integrated approach not only enhances security and transparency but also improves usability and system efficiency for real-world deployment.

III. PROPOSED SYSTEM

A. System Overview

The proposed system, **CertChain**, is a blockchain-based certificate authentication framework designed to eliminate credential fraud and enable secure, decentralized verification of academic certificates. The system integrates blockchain technology, decentralized governance, and artificial intelligence to provide a comprehensive and tamper-proof solution for certificate management.

CertChain follows a structured and secure workflow that ensures only verified institutions can issue certificates, while students and external verifiers can access and validate credentials in a transparent manner. Unlike traditional systems, which rely on centralized authorities, the proposed system leverages a decentralized architecture to remove single points of failure and enhance trust.

The system operates through a gated process consisting of institution verification, student onboarding, certificate generation, blockchain storage, and verification. Institutions are first validated through a decentralized voting mechanism, ensuring that only legitimate entities are authorized to issue certificates. Once approved, institutions can onboard students and manage academic records securely.

Students upload their academic documents, such as semester marklists, which are processed using artificial intelligence techniques for automated data extraction and validation. The system also incorporates face recognition mechanisms to ensure identity authenticity and prevent impersonation or fraudulent registrations.

After successful validation, certificates are generated as digital documents and hashed using cryptographic algorithms (SHA-256). The generated hash is stored on the Ethereum blockchain through smart contracts, ensuring immutability and tamper resistance. Secure off-chain storage mechanisms are utilized to store certificate files efficiently, while only cryptographic hashes and metadata are stored on the blockchain..

Verification is performed by comparing the cryptographic hash of a submitted certificate with the corresponding hash stored on the blockchain. Public users, such as employers or institutions, can verify certificates in real-time without requiring interaction with the issuing authority.

Overall, CertChain provides a secure, transparent, and scalable ecosystem that integrates blockchain, artificial intelligence, and decentralized governance to address the limitations of existing certificate authentication systems.

B. System Architecture

The architecture of the proposed CertChain system is designed as a multi-layered decentralized framework that integrates blockchain technology, artificial intelligence, and web- based applications to ensure secure and efficient certificate authentication.

The system consists of four primary entities: *Institutions*, *Students*, *Public Verifiers*, and the *Blockchain Network*. These entities interact through a web-based interface and backend

services, forming a complete end-to-end ecosystem for certificate issuance and verification.

1) Institutions: Institutions act as authorized certificate issuers within the system. Before issuing certificates, they must undergo a decentralized verification process through a governance voting mechanism. Once verified, institutions can onboard students, generate certificates, and record certificate data on the blockchain through smart contracts.

2) Students: Students are onboarded by verified institutions and are responsible for uploading their academic records, such as semester marklists. The system processes these documents using AI-based modules to extract and validate academic data. Students can request certificate generation and link their blockchain wallet for secure transactions.

3) Public Verifiers: Public users, such as employers or academic institutions, can verify certificates by accessing the system using a unique certificate ID. The verification process involves retrieving blockchain records and comparing cryptographic hashes to ensure authenticity without requiring interaction with the issuing authority.

4) Application Layer (Frontend and Backend): The frontend is developed using React, providing user interfaces for authentication, certificate management, and governance voting. The backend, built with Node.js and Express, handles business logic, authentication, API routing, and integration with blockchain and AI modules.

5) AI Module: The system incorporates artificial intelligence for two primary purposes: identity verification and document processing. Face recognition is used to prevent impersonation during user onboarding, while natural language processing techniques are applied to extract and validate data from uploaded marklists.

6) Blockchain Layer: The blockchain layer is implemented using the Ethereum Sepolia test network, which serves as a decentralized and tamper-resistant ledger for storing certificate-related data. Smart contracts written in Solidity are deployed to manage certificate issuance, verification, and storage operations. These contracts store essential information such as certificate identifiers, issuer details, timestamps, and cryptographic hashes. Each certificate is hashed using the SHA-256 algorithm, and the resulting hash is recorded on the blockchain through a secure transaction. This ensures im- mutability, transparency, and traceability of certificate records. Additionally, blockchain transactions require user authentication and confirmation through wallet interfaces such as MetaMask, enabling secure interaction between users and the decentralized network. Once recorded, each transaction generates a unique transaction hash that can be publicly verified using blockchain explorers, further enhancing trust and auditability. The decentralized nature of the blockchain eliminates reliance on centralized authorities and prevents unauthorized modifications or duplication of certificates.

7) Storage Layer: To optimize storage efficiency and reduce blockchain overhead, the system adopts an off-chain storage mechanism for managing certificate files and related data. Instead of storing entire certificates on the blockchain, only their cryptographic hashes and essential metadata are stored on-chain, while the actual certificate documents are securely stored in external storage systems. This hybrid storage approach significantly reduces transaction costs, improves scalability, and enhances system performance.

The off-chain storage layer ensures efficient data retrieval and management while maintaining data integrity through hash-based verification. Whenever a certificate is accessed or verified, the system recomputes its hash and compares it with the corresponding value stored on the blockchain, ensuring that the data has not been altered. This design provides a balance between decentralization and performance, enabling the system to handle large volumes of certificate data without compromising security or efficiency.

8) Governance Module: A decentralized voting mechanism is integrated into the system to validate institutions. Verified institutions participate in voting to approve or reject new applicants based on a majority rule (51% threshold), ensuring trust and preventing unauthorized entities from issuing certificates. The overall architecture ensures secure communication be- tween components, decentralized trust management, and efficient certificate verification, addressing the limitations of traditional systems.

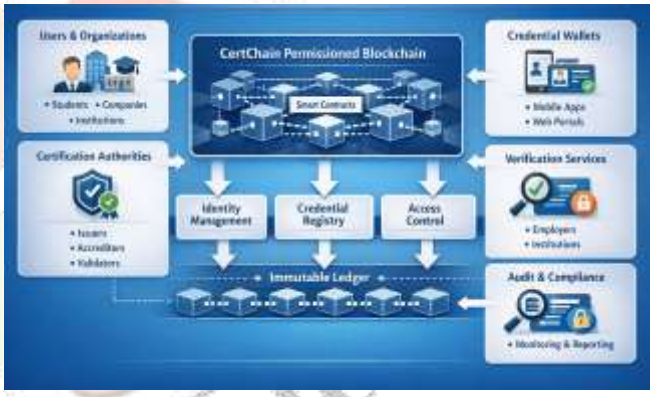

Fig. 4. Architecture of the CertChain System

C. System Modules

The CertChain system is composed of multiple interconnected modules that collectively ensure secure certificate issuance, management, and verification. Each module is de- signed to perform specific tasks within the system architecture, enabling a scalable, decentralized, and efficient certificate authentication framework.

These modules interact seamlessly to facilitate data flow between users, institutions, and the blockchain network while maintaining security and consistency. The modular design improves system flexibility, allowing individual components to be updated or extended without affecting the overall functionality. It also enhances maintainability and supports future scalability for large-scale deployments.

Furthermore, the integration of blockchain, artificial intelligence, and decentralized governance within these modules

ensures a robust and intelligent system capable of handling real-world certificate authentication challenges. Each module contributes to different stages of the certificate lifecycle, from data collection and validation to storage and verification.

1) Institution Module: The Institution Module manages the registration, verification, and operation of academic institutions within the system. Newly registered institutions are initially placed in a pending state and must undergo a decentralized governance voting process to become verified. Once approved, institutions are authorized to onboard students, issue certificates, and interact with the blockchain network. This module also handles institutional profile management, accreditation verification, and secure blockchain wallet integration for transaction signing and identity validation.

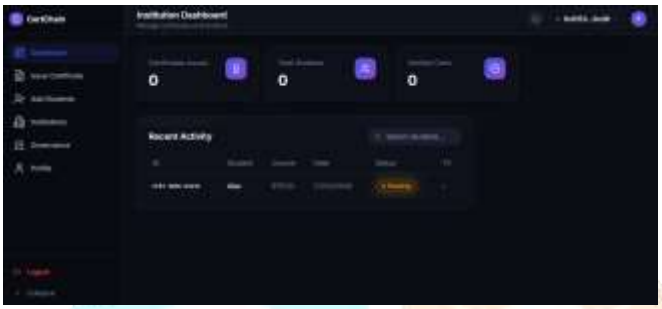

Fig. 5. Institution Dashboard Showing Certificate Management and System Activity Overview

2) Student Module: The Student Module enables students to access the system and manage their academic credentials securely. Students are onboarded by verified institutions and are provided with secure authentication credentials through role- based access control mechanisms. They can upload semester- wise marklists, verify extracted academic data, and request certificate generation. This module also supports blockchain wallet mapping, allowing secure and traceable interactions with the blockchain network.

3) Verifier Module: The Verifier Module allows external entities such as employers, organizations, or academic institutions to validate certificates in a decentralized manner. Users can input a unique certificate identifier to retrieve relevant blockchain records and associated metadata. The system verifies authenticity by recomputing and comparing the cryptographic hash of the submitted certificate with the hash stored on the blockchain, ensuring tamper-proof and real-time validation without relying on intermediaries.

4) Governance Module: The Governance Module implements a decentralized decision-making mechanism for validating institutions. Verified institutions participate in voting processes to approve or reject new applicants based on a majority rule (51% threshold). This module ensures trust, transparency, and accountability within the system while pre- venting unauthorized entities from issuing certificates. It also maintains voting records and institutional reputation within the network.

Fig. 6. Decentralized Governance Interface for Institution Verification and Voting

5) AI-Based Processing Module: The AI Module is responsible for automating identity verification and academic data extraction. It incorporates face recognition techniques to detect liveness and prevent impersonation during onboarding processes. Additionally, it utilizes document parsing and natural language processing techniques to extract structured information from uploaded marklists, such as course details, grades, and credit values. This module improves accuracy, reduces manual effort, and enhances system reliability.

6) Certificate Generation Module: This module handles the creation of digital certificates based on validated academic data. Certificates are dynamically generated in PDF format and include essential information such as student details, institution credentials, and verification identifiers. A cryptographic hash of the generated certificate is computed using the SHA-256 algorithm, ensuring data integrity before storing the hash on the blockchain.

7) Blockchain Module: The Blockchain Module is implemented using the Ethereum network and serves as the core component for ensuring data immutability and transparency. Smart contracts are deployed to manage certificate registration, validation, and storage of certificate metadata. Each certificate transaction generates a unique transaction hash, which acts as a permanent and verifiable proof of authenticity on the distributed ledger.

8) Storage Module: The Storage Module manages off-chain data storage to optimize performance and reduce blockchain costs. Certificate files and related data are stored in secure external storage systems, while only their cryptographic hashes and essential metadata are recorded on-chain. This approach improves scalability, reduces storage overhead, and ensures efficient data retrieval.

9) Notification Module: The Notification Module provides automated communication between system components and users. It generates and sends email notifications for key events such as institution registration, governance approval or rejection, student onboarding, and certificate issuance. This module enhances user experience by providing real-time updates and ensuring smooth system interaction.

Together, these modules form a cohesive, secure, and scalable system that integrates blockchain technology, artificial intelligence, and decentralized governance to provide a robust

and efficient certificate authentication solution.

IV. Methodology

The CertChain system follows a structured and secure methodology to ensure reliable certificate issuance and verification. The workflow is designed as a sequence of interconnected stages, integrating decentralized governance, artificial intelligence, and blockchain technology.

Each stage of the methodology is carefully designed to handle specific tasks, including user authentication, data extraction, certificate generation, and blockchain validation. The process begins with secure user onboarding and identity verification, followed by automated extraction and validation of academic data using AI techniques.

The validated data is then used for certificate generation, after which a cryptographic hash is created and stored on the blockchain to ensure immutability and traceability. This step-by-step approach ensures data integrity, system transparency, and efficient end-to-end certificate authentication.

Step 1: Institution Registration and Verification Institutions register within the system by providing necessary accreditation details and linking their blockchain wallet. Initially, institutions are assigned a *pending* status. A decentralized governance mechanism allows verified institutions to review and vote on new applicants. Based on a majority voting threshold (51%), institutions are either approved or rejected.

Step 2: Student Onboarding and Identity Verification Verified institutions onboard students by creating secure accounts. Students authenticate using secure credentials and map their blockchain wallets. AI-based face recognition is employed to verify identity and prevent impersonation or fraudulent registrations.

Step 3: Academic Record Submission and Processing Students upload their semester-wise marklists through the system interface. The uploaded documents are processed using document parsing and natural language processing techniques to extract structured academic data such as courses, grades, and credits. The system computes academic metrics (e.g., SGPA) and stores validated data securely.

Step 4: Certificate Generation Upon successful validation of academic records, the system generates a digital certificate in PDF format. The certificate contains student details, institutional information, and a unique certificate identifier. A cryptographic hash of the generated certificate is computed using the SHA-256 algorithm.

Step 5: Blockchain Storage The computed certificate hash is stored on the Ethereum blockchain using smart contracts. Institutions initiate blockchain transactions through Web3 wallets, and each transaction generates a unique transaction hash. This ensures immutability, transparency, and tamper resistance.

Step 6: Certificate Verification Public users, such as employers or organizations, can verify certificates by entering a certificate ID. The system retrieves the corresponding blockchain record and compares the cryptographic hash of the submitted certificate with the stored hash to validate authenticity.

Step 7: Notification and Updates The system provides automated notifications to users at various stages, including institution approval, student onboarding, and certificate issuance. This ensures seamless communication and enhances user experience.

This methodology ensures a secure, transparent, and decentralized workflow for certificate authentication, effectively addressing the limitations of traditional systems.

A. Workflow

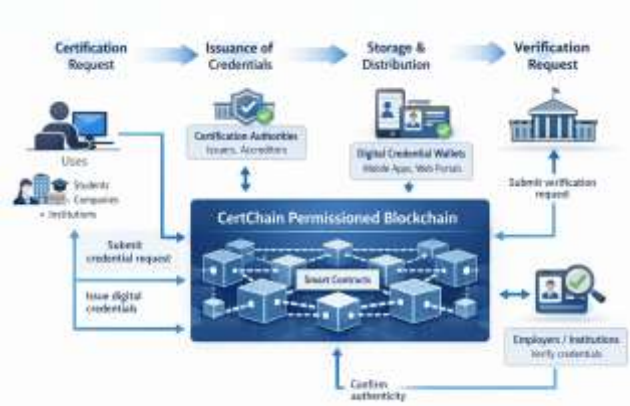

Fig. 7. Workflow of the CertChain Certificate Authentication System

V. Implementation

The CertChain system is implemented using a combination of modern web technologies, blockchain frameworks, and artificial intelligence modules to ensure secure and efficient certificate authentication. The implementation follows a layered architecture consisting of frontend, backend, blockchain, and AI components, enabling seamless interaction between users and the decentralized system.

Each layer is designed to handle specific functionalities while maintaining clear separation of concerns, improving system scalability and maintainability. The frontend layer provides an intuitive user interface for institutions, students, and verifiers, while the backend manages business logic, data processing, and secure communication. The blockchain layer ensures immutability and transparency of certificate data, and the AI components automate identity verification and academic data extraction.

The integration of these components enables a robust and reliable system capable of handling real-world scenarios with improved performance, security, and user experience. The implementation also emphasizes modularity and extensibility, allowing future enhancements and integration with emerging technologies.

A. Frontend Implementation

The frontend of the system is developed using React.js and Vite, providing a dynamic, responsive, and user-friendly interface. Tailwind CSS is used for styling, ensuring consistency and accessibility across different devices. The application is structured into modular components such as authentication interfaces, institution dashboards, student portals, and governance panels.

Key components include the certificate issuance interface, marklist upload module, and face verification interface. The frontend also incorporates real-time validation and form handling using libraries such as react-hook-form and zod. Web3 functionality is integrated using the ethers.js library, enabling users to interact with the Ethereum blockchain through Meta- Mask wallets. API communication is managed using Axios and React Query, ensuring efficient data fetching, caching, and synchronization.

Fig. 8. Frontend Interface of the CertChain System Showing Landing Page and Navigation

B. Backend Implementation

The backend is implemented using Node.js and Express, following a modular MVC architecture to ensure scalability and maintainability. It handles core functionalities such as authentication, data processing, governance logic, and blockchain interaction. MongoDB is used as the primary NoSQL database for storing user profiles, institutional records, voting data, and certificate metadata.

Authentication is secured using JSON Web Tokens (JWT) and bcrypt for password hashing. The backend exposes RESTful APIs for managing user registration, institution verification, voting operations, and certificate processing workflows. File uploads, including marklists, are handled using multer, while server-side validation ensures data consistency and integrity. Additionally, role-based access control (RBAC) is enforced to restrict actions based on user roles.

C. Blockchain Integration

The blockchain component is implemented using the Ethereum Sepolia test network to ensure decentralized and tamper-proof storage of certificate data. Smart contracts are developed in Solidity to manage certificate records, including certificate identifiers, student addresses, institution details, cryptographic hashes, and timestamps.

The ethers.js library is used for interacting with the blockchain from both frontend and backend layers. During certificate issuance, the backend computes a SHA-256 hash of the generated certificate, and the frontend initiates a transaction through the user's MetaMask wallet to store this hash on the blockchain. The resulting transaction receipt hash is stored in the database, enabling traceability and verification. This process ensures immutability and transparency in certificate management.

Each transaction is permanently recorded on the blockchain, allowing it to be publicly verified through blockchain explorers, thereby enhancing trust and auditability. Additionally, the decentralized nature of the system eliminates single points of failure and ensures that certificate data remains secure and consistently accessible.

Fig. 9. MetaMask Interface Showing User Confirmation for Blockchain Transaction

Fig. 10. Blockchain Transaction Record Showing Certificate Hash Storage on Ethereum Sepolia Network

D. AI-Based Modules

Artificial intelligence is integrated into the system for identity verification and automated document processing. The face verification module utilizes face-api.js running on TensorFlow.js to detect facial features, map facial landmarks, and generate feature vectors for identity validation. This ensures liveness detection and prevents impersonation or deepfake-based fraud. The module enhances system security by ensuring that only genuine users are allowed to access and interact with the platform.

For document processing, the system employs PDF parsing techniques to extract structured data from uploaded marklists. Libraries such as pdf-parse are used to convert PDF content

into text, which is further processed using custom parsing algorithms and regular expressions. The system extracts key attributes such as course names, grades, credits, and semester details, and automatically computes academic metrics such as SGPA. Extracted data is validated before being stored in the database.

Additionally, the AI module reduces manual effort and minimizes human errors in data entry, improving overall system efficiency. The integration of automated data extraction and verification ensures faster processing of academic records and enhances the reliability of certificate generation.

Fig. 11. AI-Based Extraction Result Showing Student Details and Computed SGPA

Fig. 12. AI-Based Academic Marklist Extraction and Data Processing Interface

E. Certificate Generation and Security

Certificates are dynamically generated using the pdf-lib library, enabling structured and customizable PDF creation. Each certificate includes essential information such as student details, institution credentials, issuance date, and a unique certificate identifier. QR codes are embedded within the certificate to enable quick verification by linking to the blockchain-based validation interface.

To ensure authenticity, certificate generation is restricted to verified institutions, and standardized templates are used to maintain consistency and prevent unauthorized modifications. The system also ensures secure handling of certificate data during generation and storage processes.

A cryptographic hash (SHA-256) of the generated certificate is computed to ensure data integrity. This hash is stored on the blockchain, making the certificate tamper-proof. Any modification to the certificate results in a hash mismatch during verification, enabling reliable detection of forged or altered documents.

Additionally, each certificate is associated with a unique blockchain transaction hash, providing traceability and enabling independent verification by third parties. This approach eliminates reliance on centralized authorities and enhances transparency. The integration of QR-based access and blockchain verification ensures real-time authentication and reduces manual verification efforts.

Fig. 13. Certificate Generation and Issuance Interface with Academic Verification

F. Notification System

The system incorporates an automated email notification module using nodemailer, configured with SMTP services. Notifications are triggered at key stages such as institution registration, governance approval or rejection, student on-boarding, and certificate issuance. These notifications include secure links and relevant information, ensuring effective communication and improving user engagement.

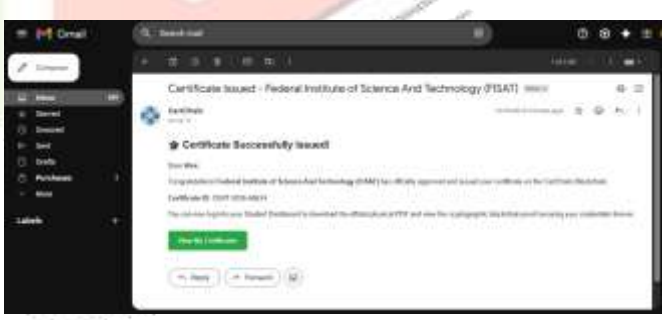

Fig. 14. Email Notification Sent to Users Upon Certificate Issuance

G. System Integration and Security Considerations

The overall system integrates multiple technologies to ensure secure and efficient operation. Secure communication is maintained using HTTPS protocols, and sensitive data is protected through encryption and hashing mechanisms. The use of RBAC, JWT authentication, and blockchain-based validation ensures that only authorized users can perform critical operations.

The integration of blockchain with off-chain storage, AI-based verification, and decentralized governance results in a

robust system capable of handling real-world certificate authentication challenges with improved security, transparency, and scalability. The system also incorporates secure API communication and input validation techniques to prevent unauthorized access and data manipulation.

Additionally, the system is designed to maintain data consistency across different components while ensuring minimal latency in operations. This coordinated integration enhances overall system performance and supports scalable deployment in real-world environments.

Overall, this integrated approach ensures a secure, efficient, and reliable framework for digital certificate authentication.

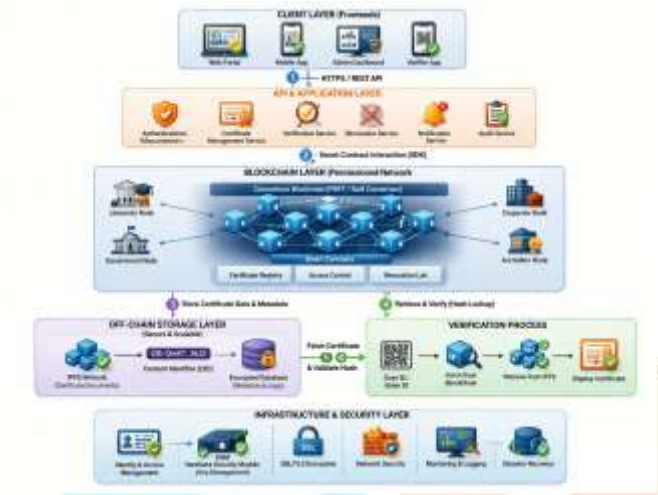

Fig. 15. Implementation Architecture of CertChain System

VI. Results and Discussion

The performance of the proposed CertChain system is evaluated based on key parameters such as security, verification efficiency, scalability, and usability. The system was tested using multiple user roles, including institutions, students, and public verifiers, to validate its real-world applicability.

A. Certificate Issuance and Verification

The system successfully enables end-to-end certificate issuance and verification. Verified institutions were able to generate certificates, which were securely hashed and stored on the Ethereum blockchain. Each certificate was associated with a unique transaction hash, ensuring traceability and immutability.

During verification, the system recomputed the hash of the uploaded certificate and matched it with the blockchain record. The results showed that any modification to the certificate resulted in a mismatch, effectively detecting tampering. This demonstrates the robustness of the system against certificate forgery.

Fig. 16. Certificate Details Interface Showing Verified Status and On-Chain Transaction Evidence

Fig. 17. Certificate Verification Result Showing Authentic Blockchain Validation

B. Performance Analysis

The integration of blockchain and off-chain storage mechanisms significantly improved system performance. By storing only cryptographic hashes on-chain and maintaining certificate files off-chain, the system reduced storage overhead and transaction costs.

Verification time was observed to be minimal, as the process involved direct hash comparison without requiring communication with issuing institutions. The decentralized nature of the system eliminates delays associated with manual verification in traditional systems.

C. Security Evaluation

The system provides multiple layers of security:

- Blockchain ensures immutability and tamper resistance.
- Cryptographic hashing (SHA-256) guarantees data integrity.
- AI-based face verification prevents impersonation and fraudulent registrations.
- Role-Based Access Control (RBAC) restricts unauthorized actions.

These combined mechanisms significantly enhance the overall security compared to traditional certificate authentication systems.

D. Comparison with Existing Systems

The proposed system was compared with traditional and existing blockchain-based solutions based on key parameters.

TABLE III
PERFORMANCE COMPARISON OF CERTIFICATE AUTHENTICATION SYSTEMS

Parameter	Traditional System	Existing Systems	CertChain
Verification Time	High	Moderate	Low
Security	Low	Moderate	High
Forgery Detection	Weak	Moderate	Strong
Transparency	Low	Moderate	High
Scalability	Limited	Moderate	High
Automation	Low	Partial	High

E. Discussion

The results demonstrate that CertChain effectively addresses the limitations of existing systems by integrating blockchain, artificial intelligence, and decentralized governance. The system eliminates dependency on centralized authorities, reduces verification time, and enhances security through cryptographic and AI-based mechanisms.

However, certain limitations remain, such as dependency on blockchain transaction fees and network latency. These challenges can be addressed in future work through optimization techniques and alternative blockchain solutions.

Overall, the proposed system provides a scalable, secure, and efficient framework for next-generation certificate authentication.

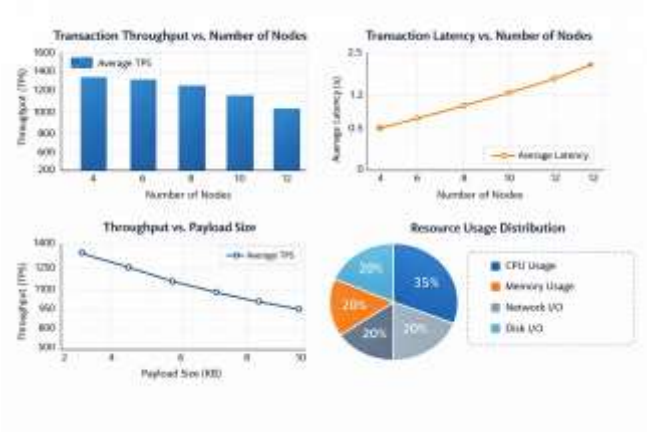

Fig. 18. Performance Analysis of CertChain System

VII. CONCLUSION

This paper presented **CertChain**, a blockchain-based certificate authentication system designed to address the limitations of traditional credential verification methods. The proposed system leverages Ethereum blockchain technology, cryptographic hashing, decentralized governance, and artificial intelligence to provide a secure, transparent, and tamper-proof solution for certificate management.

The system successfully eliminates the dependency on centralized authorities by introducing a decentralized voting mechanism for institution validation, ensuring that only trusted entities are authorized to issue certificates. The integration of AI-based modules, including face verification and automated marklist extraction, enhances the accuracy, reliability, and automation of the system while significantly reducing manual intervention and human error.

Furthermore, the use of blockchain technology ensures data immutability, transparency, and traceability, enabling real-time certificate verification through cryptographic hash comparison. The incorporation of smart contracts automates certificate issuance and validation processes, thereby improving efficiency and reducing operational overhead.

The implementation results demonstrate that CertChain significantly improves security, reduces verification time, and enhances transparency compared to existing and traditional systems. The hybrid approach of combining on-chain and off-chain storage mechanisms optimizes system performance, minimizes storage costs, and ensures scalability for large-scale deployment.

In addition, the system addresses critical challenges such as certificate forgery, unauthorized modification, and inefficient verification workflows by providing a decentralized and trustless verification framework. The inclusion of role-based access control and secure authentication mechanisms further strengthens the overall system security.

Overall, CertChain provides a robust, scalable, and intelligent framework for next-generation certificate authentication systems. By integrating blockchain, artificial intelligence, and decentralized governance, the proposed solution establishes a reliable and future-ready infrastructure for secure digital credential verification, thereby enhancing trust and integrity in academic and professional ecosystems.

Although the proposed CertChain system provides a secure and efficient solution for certificate authentication, several enhancements can be incorporated in future work to further improve its performance, scalability, and real-world applicability.

One major area of improvement is the adoption of advanced blockchain architectures. The current implementation utilizes the Ethereum Sepolia test network, which may introduce transaction costs and latency. Future work can explore the use of Layer-2 scaling solutions or alternative blockchain platforms such as Polygon or Hyperledger to reduce gas fees and improve transaction throughput.

Interoperability is another important aspect that can be enhanced. Future systems can enable cross-chain certificate verification, allowing credentials issued on different blockchain networks to be validated seamlessly. This would support global adoption and integration across multiple institutions and platforms.

The governance mechanism can also be extended by incorporating more advanced decentralized autonomous organization (DAO) models. This would allow dynamic voting policies, reputation-based voting systems, and automated governance rules to further strengthen trust and decentralization.

In terms of artificial intelligence, more sophisticated models can be integrated for improved document verification and fraud detection. For example, deep learning techniques can be used to detect forged documents or manipulated images more

accurately. Additionally, advanced biometric authentication methods, such as multi-factor or behavioral biometrics, can be incorporated to enhance user identity verification.

The system can also be extended to support a wider range of credentials beyond academic certificates, including professional certifications, licenses, and digital badges. Integration with global standards such as verifiable credentials (VCs) and decentralized identifiers (DIDs) can further improve portability and standardization.

From a usability perspective, future improvements can include mobile application support, improved user interfaces, and simplified key management solutions to enhance user adoption. Secure wallet abstraction techniques can be implemented to reduce the complexity of blockchain interactions for non-technical users.

Finally, large-scale deployment and real-world testing across multiple institutions can be conducted to evaluate system performance under realistic conditions. This would provide valuable insights into scalability, reliability, and user acceptance.

Overall, these future enhancements will further strengthen the CertChain system, making it more scalable, interoperable, and suitable for widespread adoption in secure digital credential verification.

REFERENCES

[1] https://www.ijert.org/a-survey-on-distributed-ledger-based-certificate-authentication-system-ijertv15is020182

[2] R. Priyadarshini *et al.*, "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," *IEEE Access*, vol. 13, pp. 27037–27055, 2025.

[3] A. Mondal *et al.*, "Blockchain-Based Secure E-Certificate Management System," *IEEE Access*, vol. 11, pp. 45621–45634, 2023.

[4] S. Sharma *et al.*, "Unforgeable Digi-Physical Academic Certificates," *IEEE Access*, vol. 13, 2025.

[5] R. Rahardja *et al.*, "Blockchain-Based Digital Certificate Authentication Framework," *Journal of Web Engineering*, 2024.

[6] G. Ghani *et al.*, "Permissioned Blockchain Network for Student Credentials," *IEEE Access*, 2023.

[7] A. Garba *et al.*, "Privacy-Preserving Certificate Authentication," *IEEE TIFS*, 2022.

[8] T. Nguyen *et al.*, "Decentralized Authentication for Web 3.0," *ACM Computing Surveys*, 2023.

[9] T. Merlec *et al.*, "Blockchain-Based Degree Verification," *Future Internet*, 2022.

[10] M. Turkanovic´ *et al.*, "EduCTX Platform," *IEEE Access*, 2018.

[11] K. Adja *et al.*, "Decentralized PKI Using Blockchain," *IEEE Security & Privacy*, 2020.

[12] A. Killedar and R. Joshi, "Smart Contract-Based Academic Certificates," *Blockchain: Research and Applications*, 2021.

[13] Y. Zhang *et al.*, "Secure Certificate-Based Access Control," *IEEE TNSE*, 2021.

[14] S. Lamkoti and R. Kulkarni, "Blockchain for Academic Certificates," *Education and Information Technologies*, 2022.

[15] H. Wang *et al.*, "LightLedger Certificate Authentication," *IEEE TNSE*, 2021.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.